


[Web](#) [Images](#) [Groups](#) [News](#) [Froogle](#) [more »](#)

[Advanced Search](#)
[Preferences](#)

"of" is a very common word and was not included in your search. [\[details\]](#)

Web Results 1 - 10 of about 17,000 for **k out of n secret sharing problem daterange:2449718-2451910**. (0.2

M5410 - Secret Sharing Schemes

... where there are n people involved and any k of them can obtain the **secret**. Schemes with this access structure are called **k out of n** schemes (also known as (k ...

www-math.cudenver.edu/~wcherow/courses/m5410/ctcsss.html - 8k - [Cached](#) - [Similar pages](#)

Bibliography on Secret Sharing Schemes

... Generalized ideal **secret sharing** schemes and matroids, **Problems** Infom. ... M. Krause and HU Simon, Contrast-optimal **k out of n secret sharing** schemes in visual ...

ccc.cs.lakeheadu.ca/bisss.html - 45k - [Cached](#) - [Similar pages](#)

[PS] Visual Cryptography II: Improving the Contrast Via the

File Format: Adobe PostScript - [View as Text](#)

... 2. In the Eurocrypt'94 paper (as well as in [1]) this basic model was extended into a visual variant of the **k-out-of-n secret sharing problem**: given a written ...

www.dia.unisa.it/SCN96/papers/NaSh.ps - [Similar pages](#)

[PS] PROACTIVE SECRET SHARING

File Format: Adobe PostScript - [View as Text](#)

... We assume that the adversary corrupts no more than **k out of n** ... time period, where k must be smaller than $n-2$ (this guarantees the existence of $k+1$ honest ...

www.research.ibm.com/security/pss.ps - [Similar pages](#)

[PS] IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 44, NO. 5, SEPTEMBER ...

File Format: Adobe PostScript - [View as Text](#)

... to P. i. j. 0. for $1 \leq j \leq n-k$. 4. i. j. ; i. j. 0. to P. i. j. ... 1. ;

s. 2. ; ; ; ; s. t. to obtain the **secret** s. Fig. 1. Unrestricted **t-out-of-n secret** ...

www.cs.bgu.ac.il/~beimel/Papers/without.ps - [Similar pages](#)

[PS] General Short Computational

File Format: Adobe PostScript - [View as Text](#)

... $H(K)$ is to add to the information some amount of redundancy and then to partition it into n fragments, each ... Reconstruction of f is possible **out of m** fragments ...

www.di.ens.fr/~wwwgrecc/Membres/beguina/data/beg95-1.ps - [Similar pages](#)

[PS] Determining the Optimal Contrast for Secret Sharing Schemes in ...

File Format: Adobe PostScript - [View as Text](#)

... 3 Approximation Error and Contrast In Subsection 3.1, we relate the **problem** of finding the best **k-out-of-n secret sharing** scheme to approximation **problems** of ...

eccc.uni-trier.de/eccc-reports/2000/TR00-003/Paper.ps - [Similar pages](#)

From daw@joseph.cs.berkeley.edu Fri Aug 16 22:55:31 PDT 1996 ...

... $s_{k-1} + \text{secret}$... that bound exactly, and S_{M-n} ends up containing exactly the 2^{n-1} sets ... but I think with some additional thought you can figure **out** how to ...

<http://cs.berkeley.edu/~daw/my-posts/paranoid-spy> - 9k - [Cached](#) - [Similar pages](#)

[PS] VOLUME 83, NUMBER 3 PHYSICALREVIEWLETTERS 19 JULY 1999

File Format: Adobe PostScript - [View as Text](#)

... n shares with the following two properties. First, from any ... $k-1$ or fewer shares, no information at all can ... scheme, by simply discarding (ie, tracing **out**) one of ...

www.cpsc.ucalgary.ca/~cleve/pubs/qss_prl.ps - [Similar pages](#)

[PS] Oblivious Key Escrow

File Format: Adobe PostScript - [View as Text](#)

... escrowed using some **secret-sharing** scheme [Simm92] with a very large number of shares (eg, a **k-out-of-n** threshold scheme where $k = 500$ and $n = 5000$, but ...

www.crypt0.com/papers/netescrow.ps - [Similar pages](#)

Goooooooooooooogle ►

Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2004 Google


[Web](#) [Images](#) [Groups](#) [News](#) [Froogle](#) [more »](#)

[Advanced Search](#)
[Preferences](#)

"of" is a very common word and was not included in your search. [\[details\]](#)

Web Results 21 - 30 of about 17,200 for k out of n secret sharing problem daterange:2449718-2451910. (0.:

CRYPTO '99

... This work gave two adaptive **k-out-of-n** ... Given **n** players, they defined two-phase protocols ... communications, private modular addition, or proactive **secret sharing**. ...
www.ieee-security.org/Cipher/ConfReports/1999/CR1999-crypto99.html - 70k - [Cached](#) - [Similar pages](#)
[\[More results from www.ieee-security.org \]](#)

[PS] Chinese Remaindering with

File Format: Adobe PostScript - [View as Text](#)
 ... Gamma Any **k** el'ts **out of n** specify message. - Typeset by FoilT. E. ... $n. 2 \log n$; ...
 $2n \log n$ implies. errors corrected, ($n \log k$). $1. 2+o(1)$ 1. 2. p. ...
theory.lcs.mit.edu/~madhu/slides/crt.ps - [Similar pages](#)

[PS] SOCIETY ORIENTED

File Format: Adobe PostScript - [View as Text](#)
 ... ffl Blackburn ffl Burmester ffl De Santis ffl Di Crescenzo ffl Frankel ffl Ja jodia
 ffl Yung ffl Wild Special thanks to K. Kurosawa and D ... **2-out-of-l**. ... mod **n**. 10. ...
www.cs.fsu.edu/~desmedt/lectures/society-oriented.ps - [Similar pages](#)

[PS] [13] Rabin MO, "Randomized Byzantine Generals " Proc. of 24th FOCS ...

File Format: Adobe PostScript - [View as Text](#)
 ... ciphertext **c** (that is $E(p; k) = c$). 6. ... It turns **out** that the possibility (or
 impossibility) of **secret-sharing** schemes is not based on infinity alone. ... **n**. ...
www.cs.technion.ac.il/~eyalk/CKss.ps.Z - [Similar pages](#)

3.1 Identification. 3.1.1 Computer Logins 3.1.2 Zero Knowledge ...

... prosecutors combine the shares they will find **out**, but that ... is something recognisable
 (if you see the **k** you can ... up and publishes a public RSA key (**n**,**e**). Alice ...
fringe.davesource.com/Fringe/Hacking/Cryptography/Encryption_Class/class3 - 31k - [Cached](#) - [Similar pages](#)

[DOC] Vulnerabilities introduced by mechanisms for fault tolerance

File Format: Microsoft Word 97 - [View as HTML](#)
 ... Cryptographic mechanisms exist that allow keys to be reconstructed only
 if **k out of n** holders of the **secret** combine their shares. ...
www.tolerantsystems.org/Williamsburg/TolGrpSummary.doc - [Similar pages](#)

[DOC] An Efficient Elliptic Curve Threshold Digital Signature

File Format: Microsoft Word 6
 ... In the scheme, **k out of n** signers cooperate to issue a signature without using trusted
 center. ... A (**k**, **n**) threshold **secret sharing** scheme is a protocol ...
grouper.ieee.org/groups/1363/StudyGroup/contributions/th-sche.doc - [Similar pages](#)

COCOON'97 Third Annual International Computing and Combinatorics ...

... Optimal **k out of n Secret Sharing** Schemes in Visual Cryptography --- Thomas Hofmeister,
 Matthias Krause, Hans U. Simon An algorithm for Heilbronn's **problem** --- ...
eccc.uni-trier.de/eccc/info/Conferences/COCOON97.AP.html - 6k - [Cached](#) - [Similar pages](#)
[\[More results from eccc.uni-trier.de \]](#)

Research Articles

... ER Verheul and HCA van Tilborg, Constructions and properties of **k out of n** visual
secret sharing shemes, Designs, Codes and Cryptography, 11(2), 1997 ...
www.win.tue.nl/math/eidma/jaarverslagen/verslag97/node33.html - 39k - [Cached](#) - [Similar pages](#)

[PS] Securing Threshold Cryptosystems against Chosen Ciphertext

File Format: Adobe PostScript - [View as Text](#)

... The **problem** is a bit subtle ... Basic Tools 4.1 Threshold **secret sharing** Let q be a prime, and $1 \leq k \leq n$. Shamir's [30] **k out of n secret sharing** scheme over ...

www.research.ibm.com/security/tcc.ps - [Similar pages](#)

[[More results from www.research.ibm.com](#)]

◀ GoooooooooooooooooogLe ▶

Result Page: [Previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [Next](#)

[Search within results](#) | [Language Tools](#) | [Search Tips](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2004 Google


[Web](#) [Images](#) [Groups](#) [News](#) [Froogle](#) [more »](#)

Sanguthevar Rajasekaran

Search

[Advanced Search](#)
[Preferences](#)
Web

Results 11 - 20 of about 2,550 for Sanguthevar Rajasekaran. (0.15 seconds)

Matching the bisection bound for routing and sorting on the mesh

Sponsored Links

... 15 **Sanguthevar Rajasekaran**, Randomised algorithms for packet routing on the mesh, Advances in parallel algorithms, John Wiley & Sons, Inc., New York, NY, 1992. ...

portal.acm.org/citation.cfm?id=140905 - [Similar pages](#)

[[More results from portal.acm.org](#)]

Sanguthevar Rajasekaran
 Used, New & Out-Of-Print Books.
 Find it at Alibris and Save!
www.alibris.com

[See your message here...](#)

Arrays with reconfigurable optical buses by Sanguthevar ...

Talk abstract: Arrays with Reconfigurable Optical Buses. **Sanguthevar Rajasekaran**, University of Florida. An Array with Reconfigurable ...

www.ima.umn.edu/hpc/wkshp_abstracts/rajasekaran1.html - 13k - [Cached](#) - [Similar pages](#)

Webbib References for Sanguthevar Rajasekaran

Webbib References for **Sanguthevar Rajasekaran**. lim:icc03 Jaeyong Lim and **Sanguthevar Rajasekaran**. Parallel Cache Management Protocol ...

www.cs.wpi.edu/cgi-bin/webbib/GetRefs.cgi?authorstr=%22rajasekaran,s%22 - 3k -

[Cached](#) - [Similar pages](#)

Books Written By Sanguthevar Rajasekaran - Textbook Land

... **Rajasekaran**. Computer Algorithms Psuedocode Ellis Horowitz, **Sanguthevar Rajasekaran** 15 August, 1997 ISBN: 0716783169, Picture of Book. ...

www.textbookland.com/author/Sanguthevar+Rajasekaran - 18k - [Cached](#) - [Similar pages](#)

Sanguthevar Rajasekaran

UTC Chair Professor of CSE and Director of GE E-Engg. Clinic. RESEARCH INTERESTS: I conduct research in the area of Applied Algorithms. ...

www.cse.uconn.edu/~rajasek/mainpage.htm - 2k - [Cached](#) - [Similar pages](#)

Sanguthevar Rajasekaran

Sanguthevar Rajasekaran. 257 ITE Building, 371 Fairfield Road. Dept. of CSE, Univ. of Connecticut. Storrs, CT 06269-3155. (860) 486 2428; 486 4817 (fax). ...

www.cse.uconn.edu/~rajasek/ContactInfo.htm - 3k - [Cached](#) - [Similar pages](#)

[[More results from www.cse.uconn.edu](#)]

DBLP: David SL Wei

... 2003. 24, EE, David SL Wei, **Sanguthevar Rajasekaran**, Kshirasagar Naik, Sy-Yen Kuo: Efficient Algorithms For Selection And Sorting Of Large Distributed Files On ...

www.informatik.uni-trier.de/~ley/db/indices/a-tree/w/Wei:David_S=_L=.html - 17k -

[Cached](#) - [Similar pages](#)

[[More results from www.informatik.uni-trier.de](#)]

Sanguthevar Rajasekaran

name university year home submit about help **Sanguthevar Rajasekaran**. Doctorate from Harvard University in 1987 Adviser: John Reif Students: None reported ...

sigact.acm.org/cgi-bin/genealogy.cgi?file=database-R.html&from=Rajasekaran,Sanguthevar - 3k -

[Cached](#) - [Similar pages](#)

CSE Research

... Chun-Hsi Huang. Ion Mandoiu. **Sanguthevar Rajasekaran**. Dong-Guk Shin. ... Reda Ammar. Ian GreenShields. **Sanguthevar Rajasekaran**. Distributed & Realtime Systems IDIS Lab ...

www.engr.uconn.edu/cse/cse_research.htm - 22k - [Cached](#) - [Similar pages](#)

[[More results from www.engr.uconn.edu](#)]

Optimal and Sublogarithmic Time Randomized Parallel Sorting ...

Optimal and Sublogarithmic Time Randomized Parallel Sorting Algorithms (1989) (Make Corrections) (45 citations) **Sanguthevar Rajasekaran**, John H. Reif. ...

citeseer.ist.psu.edu/rajasekaran89optimal.html - 23k - [Cached](#) - [Similar pages](#)

[[More results from citeseer.ist.psu.edu](#)]



Result Page: [Previous](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [Next](#)

[Search within results](#) | [Language Tools](#) | [Search Tips](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2004 Google


[Web](#) [Images](#) [Groups](#) [News](#) [Froogle](#) [more »](#)

[Advanced Search](#)
[Preferences](#)

Web

 Results 1 - 10 of about 52 for **Sanguthevar Rajasekaran secret sharing**. (0.20 seconds)

Sanguthevar Rajasekaran

 ... checking, random variate generation (computer simulations), optimization, cryptography (authorization, authentication, **secret sharing**), particle simulations ...

www.cse.uconn.edu/~rajasek/mainpage.htm - 2k - [Cached](#) - [Similar pages](#)

On key distribution via true broadcasting

 ... 6 Capocelli, R., De Santis, A., Gargano, L., Vactaro, U., "On the Size of **Shares** for **Secret Sharing** Schemes", Advances in Cryptology: Proceedings of CRYPTO '91 ...
portal.acm.org/citation.cfm?id=191195&jmp=citings&dl=GUIDE&dl=ACM&CFID=11111111&CFTOK... - Supplemental Result - [Similar pages](#)

On key distribution via true broadcasting

 ... 6 Renato M. Capocelli, Alfredo De Santis, Luisa Gargano, Ugo Vaccaro, On the Size of **Shares** for **Secret Sharing** Schemes, Proceedings of the 11th Annual ...
portal.acm.org/citation.cfm?id=191195 - [Similar pages](#)
[\[More results from portal.acm.org \]](#)

SPECIAL ISSUE ON RANDOMIZED COMPUTING

 ... **SANGUTHEVAR RAJASEKARAN** and SARTAJ K. SAHNI. Department of Computer and Information Science and Engineering ... Sun's paper deals with the problem of **secret sharing**. ...

www.worldscinet.com/ijfcs/11/1102/S0129054100000120.html - 6k - [Cached](#) - [Similar pages](#)

International Journal of Foundations of Computer Science

 ... SPECIAL ISSUE ON RANDOMIZED COMPUTING **Sanguthevar Rajasekaran** and Sartaj K. Sahni, ...
 ON THE DEALER'S RANDOMNESS REQUIRED IN PERFECT **SECRET SHARING** SCHEMES WITH ...

www.worldscinet.com/ijfcs/11/1102/S01290541001102.html - 6k - [Cached](#) - [Similar pages](#)

IEEE Transactions on Parallel and Distributed Systems, Vol. 9

 ... Applications & Algorithms: **Sanguthevar Rajasekaran**, Sartaj Sahni: Randomized Routing, Selection ... Wool: Access Control and Signatures via Quorum **Secret Sharing**. ...

www.sigmod.org/sigmod/dblp/db/journals/tpds/tpds9.html - 51k - [Cached](#) - [Similar pages](#)

International Journal of Foundations of Computer Science, Volume ...

 ... Randomized Computing: **Sanguthevar Rajasekaran**, Sartaj Sahni: Special Issue on Randomized ...
 the Dealer's Randomness Required in Perfect **Secret Sharing** Schemes with ...

www.sigmod.org/sigmod/dblp/db/journals/ijfcs/ijfcs11.html - 10k - [Cached](#) - [Similar pages](#)

IEEE Transactions on Parallel and Distributed Systems, September ...

 ... Routing, Selection, and Sorting on the OTIS-Mesh **Sanguthevar Rajasekaran**, Sartaj Sahni. ... 909-922 Access Control and Signatures via Quorum **Secret Sharing** Moni Naor ...

csdl.computer.org/comp/trans/td/1998/09/19toc.htm - 28k - [Cached](#) - [Similar pages](#)

The Bit Extraction Problem or t-Resilient Functions - Chor ...

 ... 1989) (Correct) 0.5: Randomized Parallel Computation - **Sanguthevar Rajasekaran** Dept (Correct ... 1984 1 How to Implement Verifiable **Secret Sharing** and Simultaneous ...

citeseer.ist.psu.edu/chor85bit.html - 20k - [Cached](#) - [Similar pages](#)

International Journal of Foundations of Computer Science

 ... by: **Sanguthevar Rajasekaran**, Sartaj Sahni v. 11 i. 2 p. 205 - 205. A Method ... On the

Dealer's Randomness Required in Perfect **Secret Sharing** Schemes with Access ...
wotan.liu.edu/docis/dbl/ijfocs/ - 101k - [Cached](#) - [Similar pages](#)

GoooogLe ►

Result Page: 1 2 3 4 **Next**

Sanguthevar Rajasekaran secret

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2004 Google


[Web](#) [Images](#) [Groups](#) [News](#) [Froogle](#) [more »](#)

[Advanced Search](#)
[Preferences](#)

Web Results 1 - 10 of about 28 for "k out of n" cryptosystem daterange:2449718-2451910. (0.28 seconds)

Descriptions of Key Escrow Systems

... can be split and escrowed using an "n out of n" or "k out of n" verifiable secret ...

The techniques apply to the RSA public key **cryptosystem** or to any single-key ...

www.cosc.georgetown.edu/~denning/crypto/Appendix.html - 101k - [Cached](#) - [Similar pages](#)

[PS] Securing Threshold Cryptosystems against Chosen Ciphertext

File Format: Adobe PostScript - [View as Text](#)

... Any practical **k out of n cryptosystem** should be robust, ie, it should be able to tolerate the presence of an adversary that tries to hinder the recovery process ...

www.research.ibm.com/security/tcc.ps - [Similar pages](#)

[doc] An Efficient Elliptic Curve Threshold Digital Signature

File Format: Microsoft Word 6

... In the scheme, **k out of n** signers cooperate to issue a signature without using ... An efficient (k, n) threshold ElGamal type public key **cryptosystem** was shown by ...

grouper.ieee.org/groups/1363/ StudyGroup/contributions/th-sche.doc - [Similar pages](#)

[PS] Issuing Sc

File Format: Adobe PostScript

... In the scheme, **k out of n** signers cooperate to issue a signature without using trusted ... n) threshold ElGamal type public key **cryptosystem** was shown by Desmedt and ...

grouper.ieee.org/groups/1363/ StudyGroup/contributions/th-sche.ps - [Similar pages](#)

Bibliography on Secret Sharing Schemes

... M. Krause and HU Simon, Contrast-optimal **k out of n** secret sharing schemes in ... in designing the conference key distribution **cryptosystem**, Information Processing ...

ccc.cs.lakeheadu.ca/bisss.html - 45k - [Cached](#) - [Similar pages](#)

[PS] Oblivious Key Escrow

File Format: Adobe PostScript - [View as Text](#)

... We give here a non-probabilistic **k-out-of-n** oblivious multicast protocol, based on blind ... k copies of the message (using a symmetric-key **cryptosystem**), with a ...

www.crypto.com/papers/netescrow.ps - [Similar pages](#)

[PS] Decentralized Trust Management

File Format: Adobe PostScript - [View as Text](#)

... Any public key **cryptosystem** can be used; signature verification on credentials ... filters that implement complex requirements, such as **k-out-of-n** threshold schemes ...

www.crypto.com/papers/policymaker.ps - [Similar pages](#)

CRYPTO '99

... The general idea was to measure the power usage of a **cryptosystem**, eg, when ... This work gave two adaptive **k-out-of-n** constructions, one based on DDH and one ...

www.ieee-security.org/Cipher/ ConfReports/1999/CR1999-crypto99.html - 70k - [Cached](#) - [Similar pages](#)

Twelfth IEEE Computer Security Foundations Workshop (CSFW12) ...

... of timing attacks on a protocol (or on the underlying **cryptosystem**) is usually ... principals; this notion can be used to represent **k-out-of-n** threshold schemes. ...

www.ieee-security.org/Cipher/ ConfReports/1999/CR1999-csfw99.html - 27k -

[Cached](#) - [Similar pages](#)

[PS] Constructions and Bounds for

File Format: Adobe PostScript - [View as Text](#)

... by Naor and Shamir [8]. They analyzed the case of **k out of n** visual cryptography ...

2 visual cryptography scheme can be thought of as a private key **cryptosystem**. ...

www.cacr.math.uwaterloo.ca/~dstinson/papers/ICALP96.ps - [Similar pages](#)

Google ►

Result Page: 1 2 3 [Next](#)

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2004 Google


[Web](#) [Images](#) [Groups](#) [News](#) [Froogle](#) [more »](#)

multi-secret threshold daterange:2449718-

Search

[Advanced Search](#)
[Preferences](#)
WebResults 1 - 10 of about 25 for **multi-secret threshold daterange:2449718-2451910**. (0.60 seconds)**[PDF] Multisecret threshold schemes**File Format: PDF/Adobe Acrobat - [View as HTML](#)

Page 1. Page 2. Page 3. Page 4. Page 5. Page 6. Page 7. Page 8. Page 9. Page 10.

dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C93/126.PDF - [Similar pages](#)**Advances in Cryptology - Crypto '93**... Vaccaro, U. **Multisecret threshold** schemes, Jackson, WA, Martin, KM and O'Keefe, CM; Secret sharing made short, Krawczyk, H. A subexponential ...dsns.csie.nctu.edu.tw/research/crypto/HTML/C93.HTM - 6k - [Cached](#) - [Similar pages](#)[[More results from dsns.csie.nctu.edu.tw](#)]**Bibliography on Secret Sharing Schemes**... Santis, G. Di Crescenzo, A. Giorgio Gaggia and U. Vaccaro, **Multi-secret** sharing schemes ... WA Jackson, KM Martin and CM O'Keefe, **Multisecret threshold** schemes, in ...ccc.cs.lakeheadu.ca/bisss.html - 45k - [Cached](#) - [Similar pages](#)**[PS] Bibliography on Secret Sharing Schemes**File Format: Adobe PostScript - [View as Text](#)... **Multi-secret** sharing schemes, in "Advances in Cryptology - CRYPTO '94", YG Desmedt, ed ... 133. WA Jackson, KM Martin and CM O'Keefe, **Multisecret threshold** schemes, ...www.cacr.math.uwaterloo.ca/techreports/1998/corr98-50.ps - [Similar pages](#)**[PS] This is a Chapter from the Handbook of Applied Cryptography, by A. ...**File Format: Adobe PostScript - [View as Text](#)... patent, 644, 659 **Multi-secret threshold** scheme, 527 Multiple encryption, 234-237. definition of, 234 double encryption, 234 modes of operation, 237. ...www.cacr.math.uwaterloo.ca/hac/about/index.ps - [Similar pages](#)[[More results from www.cacr.math.uwaterloo.ca](#)]**[PS] COMPUTING FUNCTIONS OF A SHARED SECRET AMOS BEIMEL**File Format: Adobe PostScript - [View as Text](#)... **secret** sharing schemes, in Advances in Cryptology - CRYPTO '94, Y. Desmedt, ed ... [23] W. Jackson, KM Martin, and CM O'Keefe, **Multisecret threshold** schemes, in ...www.cs.bgu.ac.il/~beimel/Papers/BBDK.ps - [Similar pages](#)**[PDF] A Secure Key Registration System Based on Proactive Secret-Sharing ...**

File Format: PDF/Adobe Acrobat

... $X=\{x_1, \dots, x_k\}$ through a $(t-k+1, t+1; k, n)$ -**multi-secret-sharing** scheme. ... keys) in or retrieve them from the system in a $(t+1, n)$ -**threshold** scheme without ...doi.ieeecs.org/10.1109/ISADS.1999.838438 - [Similar pages](#)**[PS] On-line Secret Sharing**File Format: Adobe PostScript - [View as Text](#)... 2. B. Blakley, GR Blakley, AH Chan, and JL Massey, **Threshold**. ... C. Blundo, A. De Santis, G. Di Crescenzo, AG Gaggia, and U. Vaccaro, **Multi-secret** sharing schemes ...ftp.se.kde.org/pub/security/docs/cryp/ETHZ/Online_Secret_Sharing.ps - Supplemental Result - [Similar pages](#)**[PS] Computer and Communications**File Format: Adobe PostScript - [View as Text](#)... are the medical and administrative parts of hospital records, name and salary information on payrolls, and key fragments in **threshold** signature schemes. ...www.formation.jussieu.fr/ars/2000-2001/UNIX/cours/5/COMPLEMENTS/DOC/why-cryptosystems-fail/SRV2no4.ps - Supplemental Result - [Similar pages](#)

[ps] PROACTIVE SECRET SHARING

File Format: Adobe PostScript - [View as Text](#)

... 2 Z. q. using a k-**threshold** Shamir's secret sharing: Each P. i. ... (r) (mod q). Secrecy:

The semantic security of the secret x is preserved. 18. **Multi-Secret** Sharing ...

www.research.ibm.com/security/pss.ps - [Similar pages](#)

Google ►

Result Page: 1 2 [Next](#)

[Search within results](#) | [Language Tools](#) | [Search Tips](#) | [Dissatisfied? Help us improve](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2004 Google